International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 9 Issue 5, Sep-Oct 2025 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Rising Threats and Next-Generation Defenses in Cybersecurity

Nikunj Doshi

Northeastern University, Boston, MA, USA

ABSTRACT

The cybersecurity domain is undergoing rapid transformation as artificial intelligence, quantum computing, and globally connected devices dramatically widen the digital attack surface. This study examines the principal trends in reshaping the threat environment and assesses the defensive measures organizations are adopting to address escalating risks. Using recent breach data and illustrative case studies, the analysis identifies eight critical emerging threats—including AI-driven intrusions, supply-chain compromises, and the pending disruption of post-quantum cryptography, together with counterstrategies such as zero-trust implementation, adaptive security models, and secure-by-design development practices. Key research deficits are highlighted in areas like adversarial AI, neuromorphic hardware protection, and harmonization of international regulatory frameworks. The paper concludes with practical guidance for industry professionals, academic researchers, and policymakers, stressing the importance of workforce upskilling, continuous threat-exposure management, and cross-border collaboration. By integrating technological, organizational, and policy viewpoints, this work offers a strategic roadmap for reducing cyber risk and safeguarding critical infrastructure in the coming decade.

KEYWORDS: *Cybersecurity trends; Artificial intelligence attacks; Zero-trust architecture; post-quantum cryptography; Cybersecurity governance.*

How to cite this paper: Nikunj Doshi "Rising Threats and Next-Generation Defenses in Cybersecurity" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-9 | Issue-5, October 2025, pp.531-537, URL: www.ijtsrd.com/papers/ijtsrd97555.pdf

IJTSRD97555

Copyright © 2025 by author (s) and International Journal of Trend in Scientific Research and Development Journal. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0) (http://creativecommons.org/licenses/by/4.0)

1. INTRODUCTION

Cybersecurity has always been an evolving discipline, yet the rate of transformation in recent years has been exceptional. As digital infrastructures increasingly underpin economic, social, and political activities, the overall attack surface has expanded in ways that challenge long-standing defense models (Jariwala, 2025). Emerging technologies such as artificial intelligence, quantum computing, and highly interconnected devices are reshaping not only how organizations function but also how adversaries design and execute their operations. This rapidly shifting environment brings both new opportunities and heightened risks, providing the impetus for the analysis presented in this study.

Staying ahead of the threat curve is no longer an option reserved for large enterprises; it has become a necessity for governments, companies of every size, and individual users alike. Modern breaches impose financial damages that extend far beyond immediate remediation, including the loss of intellectual property, erosion of brand reputation, and costly regulatory penalties. Lawmakers worldwide have responded with a dense array of data-protection rules and cybersecurity directives, creating additional legal obligations on top of formidable technical challenges. For security leaders, this convergence of economic stakes and regulatory oversight underscores the need for relentless vigilance and continuous adaptation.

The sections that follow interpret the term “latest trends” in a broad and integrative manner. Trends are not confined to new exploits or software flaws; they also encompass policy developments, evolving attacker behaviors, and the rise of innovative defensive paradigms. The objective is to present a wide-angle analysis that connects technological breakthroughs, threat-actor strategies, and governance dynamics, enabling readers to understand how these elements intersect to shape the modern cybersecurity landscape.

2. Today's Cybersecurity Threat and Defense Landscape

In recent years, mounting empirical evidence has made one fact unmistakable: cyber risk is rising in both frequency and financial impact. The 2025 IBM Cost of a Data Breach Report notes that while the global average breach cost dipped slightly to roughly US $4.44 million, the U.S. average climbed to about US $10.22 million per incident, a surge driven largely by regulatory penalties as well as detection and escalation expenses (IBM & Ponemon Institute, 2025; IBM, 2025a). Healthcare remains the costliest sector, with average breach expenses around US $7.42 million despite a modest decline from previous years (IBM & Ponemon Institute, 2025; HIPAA Journal, 2025). Breach lifecycles also remain troublingly long: in 2025 the global mean time from initial compromise to full containment hovered near 241 days, while healthcare organizations required more than 279 days on average (HIPAA Journal, 2025; IBM & Ponemon Institute, 2025).

Recent incidents further reveal how attackers exploit increasingly complex vectors, particularly through third-party integrations. A prominent example is the Salesloft-Drift compromise, a supply-chain intrusion that impacted over 700 organizations worldwide. In this case, adversaries stole OAuth tokens from Salesloft's Drift integrations, granting access to sensitive data housed in Salesforce, Google Workspace, and other platforms. Exfiltrated information included business contact details, customer support histories, and account metadata (Google Threat Intelligence Group; Mandiant; Trustwave; Microsoft Law Firm Report, 2025). This episode highlights how vulnerabilities can spread laterally across the trusted relationships embedded within SaaS ecosystems.

Despite these warning signs, many enterprises still rely on traditional defensive models that are proving inadequate. Heavy dependence on perimeter firewalls, signature-based intrusion detection, and compliance checklists keeps organizations reactive instead of proactive. Zero-day exploits, supply-chain intrusions, and adversaries leveraging AI for phishing and impersonation continue to outpace defenses built for older threat paradigms. Legacy systems, understaffed security teams, and tight budgets leave smaller or less mature firms especially exposed.

3. Evolving Threat Landscape

The cybersecurity threat landscape has moved from steady evolution to abrupt disruption. Attackers now combine automation, artificial intelligence, and intricate supply-chain dependencies to exploit weaknesses at unprecedented speed. The eight trends below represent the most critical developments security professionals must address.

3.1. AI-Powered and AI-Assisted Attacks

Artificial intelligence has shifted from serving mainly as a defensive capability to functioning as an offensive weapon. Generative models are leveraged to craft convincing phishing emails, counterfeit documents, and deepfake videos that evade traditional detection mechanisms. Losses from deepfake-related fraud surpassed US $200 million in North America in just the first quarter of 2025, and more than half of surveyed companies in the United States and United Kingdom reported at least one attempted deepfake scam within the past year (World Economic Forum, 2025).

AI is also accelerating the discovery of vulnerabilities. Machine-learning agents can comb through codebases, uncover zero-day flaws, and generate exploit scripts far faster than human analysts (CrowdStrike, 2025). Autonomous agents capable of chaining reconnaissance, credential harvesting, and lateral movement are beginning to circulate on underground forums. A recent example involved misuse of Anthropic's Claude model to design phishing campaigns and malicious code before internal safeguards intervened (Reuters, 2025).

3.2. Supply Chain Vulnerabilities

Modern organizations rely on multiple tiers of third-party vendors, open-source components, and interconnected devices. A single weakness in this chain can cascade downstream. The 2025 Salesloft-Drift breach, which exposed data from hundreds of Salesforce customers through a compromised integration, demonstrates how one vendor's vulnerability can disrupt entire ecosystems (Trustwave, 2025). Open-source repositories, firmware updates, and Internet-of-Things (IoT) hardware remain frequent targets because security oversight is uneven and patch cycles are often delayed (Cybersecurity Dive, 2025).

3.3. Zero-Trust, Identity, and Access Management Evolutions

As networks become increasingly distributed, identity now serves as the new security perimeter. Organizations are tightening least-privilege policies, implementing continuous verification of users and devices, and deploying adaptive access controls that evaluate behavioral anomalies and device health. Although zero-trust frameworks are widely promoted, real-world adoption remains uneven, and many enterprises struggle to integrate identity governance into legacy systems (IBM Security, 2025).

3.4. Post-Quantum Cryptography

Quantum computing poses an existential threat to current encryption methods. Adversaries can harvest encrypted data today and store it until large-scale quantum computers make decryption feasible. Both the European Union and the U.S. National Institute of Standards and Technology (NIST) have issued guidance urging critical-infrastructure operators to implement quantum-resistant algorithms by decade's end (Eraneos, 2025; IndustrialCyber, 2025). Developing "crypto agility"—the ability to swap cryptographic primitives quickly—is emerging as a required capability rather than a theoretical best practice.

3.5. Regulatory, Ethical, and Policy-Driven Trends

Governments are responding to growing cyber risk with more stringent compliance mandates. In Europe, the NIS2 Directive, the Cyber Resilience Act, and the Digital Operational Resilience Act require stronger risk-management controls, supply-chain protections, and rapid incident reporting (ENISA, 2025). Similar measures are advancing across North America and Asia. Alongside these policies, ethical concerns—such as AI bias, privacy infringement, and accountability for algorithmic decision-making—remain dominant topics in global forums (World Economic Forum, 2025).

3.6. Continuous Threat Exposure and Monitoring

Periodic audits and scheduled penetration tests are no longer sufficient. Leading enterprises are adopting continuous threat-exposure management that integrates real-time analytics, automated detection and response, and ongoing red-team exercises designed to simulate evolving attacker tactics. This proactive approach shortens dwell time and enables faster mitigation of new vulnerabilities (IBM Security, 2025).

3.7. Edge, IoT, and Neuromorphic Computing Threats

The rapid spread of IoT devices and edge-computing nodes dramatically expands the attack surface. Many devices lack secure update mechanisms or even basic hardening, making them attractive entry points for ransomware groups and botnet operators (Cybersecurity Dive, 2025). Neuromorphic computing—hardware engineered to emulate neural processes—introduces further uncertainty. Early research indicates susceptibility to mimicry and side-channel attacks, yet standardized safeguards have not been established.

3.8. Workforce and Skills Trends

Technology alone cannot protect organizations without skilled professionals to design and manage defenses. The global cybersecurity workforce shortage exceeded four million positions in 2025, with particularly acute gaps in AI security, post-quantum cryptography, and regulatory compliance (ISC², 2025). Cross-disciplinary expertise spanning software engineering, data science, and policy is increasingly vital. Organizations that fail to invest in talent development risk being outpaced by adversaries who face no comparable constraints.

4. Modern Cyber Defense and Response Strategies

As cyber threats become more sophisticated, defensive approaches are shifting from static safeguards to dynamic, intelligence-driven ecosystems. Organizations are increasingly investing in tools and processes that shorten detection times, automate remediation, and weave security into every stage of the technology lifecycle. Five major developments illustrate this evolution.

4.1. AI and Machine Learning for Defense

Artificial intelligence has moved beyond experimental use and now plays a central role in threat detection and incident response (Bhatt, 2024). AI-driven threat-intelligence platforms aggregate massive volumes of network telemetry, dark-web activity, and behavioral indicators to spot anomalies almost in real time (IBM Security, 2025). Machine-learning models learn the normal rhythm of network activity and can flag subtle deviations that indicate lateral movement or insider compromise. Automation enables these systems to recommend or even execute containment actions before human analysts can react. Large language models (LLMs) are also being adapted for defensive functions such as vulnerability discovery, secure code review, and automated reporting. Early deployments show that LLMs can cut the time needed to triage vulnerability disclosures and improve the precision of patch recommendations (Microsoft Security, 2025). At the same time, defenders must remain vigilant against adversarial manipulation of these models, which can create false positives or biased outputs.

4.2. Zero-Trust Architectures

Zero trust has matured from a conceptual idea into a practical blueprint for enterprise protection. Instead of assuming that internal network traffic is trustworthy, zero-trust models verify every access request regardless of origin. Implementation typically involves continuous authentication, granular network micro-segmentation, and policy engines that evaluate device posture and user behavior before access is

granted (National Institute of Standards and Technology [NIST], 2023). Organizations adopting zero-trust principles report shorter breach lifecycles and lower remediation costs compared with traditional perimeter-based approaches (IBM & Ponemon Institute, 2025).

4.3. Adaptive Security and Real-Time Systems

Because attackers continually modify their tactics, defensive measures must adapt just as quickly. Adaptive security frameworks integrate continuous monitoring, predictive analytics, and dynamic policy enforcement to adjust controls in response to evolving threats (Gartner, 2024). Examples include firewalls that retrain on live traffic to recognize new exploit signatures, moving-target defenses that alter network configurations to frustrate reconnaissance, and automated isolation of compromised workloads in cloud environments. These capabilities are designed to disrupt the attacker's decision cycle and reduce the time between detection and response from hours to seconds.

4.4. Secure by Design and DevSecOps

Integrating security at the earliest stages of system development is now viewed as essential. The secure-by-design movement encourages hardware and software vendors to incorporate security features and threat modeling into initial design specifications rather than adding them later (Cybersecurity and Infrastructure Security Agency [CISA], 2023). DevSecOps practices support this approach by uniting development, security, and operations teams to automate code scanning, dependency checks, and continuous integration/continuous deployment (CI/CD) pipeline testing.

Open-source auditing is particularly critical because many modern applications depend on shared libraries whose vulnerabilities can spread widely, as seen in the Log4j incident. Organizations that implement automated software-composition analysis report significant reductions in exposure windows for newly disclosed vulnerabilities (Synopsys, 2025).

4.5. Regulation, Compliance, and Governance

Governments and industry groups are strengthening cybersecurity through more rigorous regulatory frameworks. New and revised standards mandate timely incident reporting, secure product design, and regular third-party audits. The European Union's Cyber Resilience Act requires baseline security for hardware and software products sold in the EU, while the U.S. Cyber Incident Reporting for Critical Infrastructure Act compels critical operators to disclose breaches within specified time frames (European Commission, 2024; U.S. Cybersecurity and Infrastructure Security Agency [CISA], 2023). Certification schemes such as ISO/IEC 27001 and SOC 2 remain influential, but regulators increasingly demand continuous assurance rather than periodic attestations. These governance mechanisms exert external pressure on organizations to maintain robust controls while also providing a framework for internal accountability. Boards of directors are now expected to oversee cyber-risk management, and failure to meet these expectations can result in regulatory penalties and reputational harm (PwC, 2025).

5. Challenges and Existing Research Gaps

Even as defensive technologies advance, several unresolved issues continue to impede progress. These obstacles span technical design, legal and policy frameworks, human behavior, and economic constraints, leaving ample room for future research.

5.1. Technical Challenges

The rapid integration of artificial intelligence and machine learning into cybersecurity brings new layers of complexity. Models trained on massive, heterogeneous datasets often function as "black boxes," making it difficult to interpret or audit their decisions (Goodman et al., 2024). This lack of transparency raises accountability concerns when automated systems mistakenly block legitimate traffic or fail to detect an intrusion. Scalability presents another problem: algorithms that perform well in controlled laboratory settings frequently degrade when deployed across global networks processing billions of events per day (IBM Security, 2025). Persistent false positives and false negatives further erode analyst confidence and consume limited resources.

Securing heterogeneous, distributed infrastructures is equally challenging. Edge-computing nodes, IoT devices, and experimental neuromorphic processors introduce diverse hardware and software stacks, each with unique vulnerabilities and patching requirements. Achieving consistent security policies across these environments demands orchestration and verification techniques that current tools cannot fully deliver.

5.2. Policy, Legal, and Ethical Issues

Regulatory and legal frameworks often lag behind technological innovation. Policymakers struggle to balance strong security measures with privacy protections, especially when continuous monitoring and behavioral analytics are employed (European Data Protection Board [EDPB], 2024). Cross-border data flows complicate enforcement because attackers exploit jurisdictional gaps. Governance of AI in adversarial contexts remains unsettled: questions persist over liability when a defensive AI system

causes collateral damage and over how international treaties should address the development of offensive AI capabilities (World Economic Forum, 2025).

5.3. Usability and Human Factors

Despite advances in technology, humans remain the weakest link. Social-engineering campaigns consistently circumvent technical defenses by exploiting trust, distraction, or fatigue. Training programs can reduce—but never fully eliminate—human error, and user awareness typically declines over time (Verizon, 2025). Designing interfaces and workflows that encourage secure behavior without creating excessive friction continues to pose a significant research challenge.

5.4. Economic and Organizational Constraints

Cybersecurity budgets rarely grow in proportion to rising risks. Small and medium-sized enterprises face severe financial pressures and often postpone critical upgrades, leaving legacy systems exposed (PwC, 2025). Even large organizations struggle to recruit qualified professionals, with the global cybersecurity workforce gap surpassing four million positions in 2025 (ISC², 2025). Limited resources force organizations to make difficult trade-offs between immediate operational needs and long-term security investments.

6. Illustrative Cases and Real-World Scenarios

Recent breaches demonstrate how the previously discussed challenges converge in real-world scenarios and reveal both the strengths and weaknesses of current defensive measures.

6.1. MOVEit Incident: A Major Supply-Chain Compromise

Beginning in mid-2023 and extending into 2024, attackers exploited a zero-day vulnerability in Progress Software's MOVEit file-transfer platform, stealing data from more than 2,600 organizations worldwide, including government agencies and Fortune 500 companies (Coveware, 2024). The incident illustrates the cascading nature of third-party risk: once a trusted service was compromised, sensitive information from downstream customers was exfiltrated. Many affected organizations depended heavily on perimeter firewalls and periodic vendor assessments, defenses that proved insufficient against a trusted integration. Response times varied widely. Companies employing continuous threat-exposure management isolated compromised servers within hours, while others took weeks to detect the intrusion, highlighting the value of real-time monitoring and well-practiced incident-response procedures.

6.2. MGM Resorts Attack: A Modern Ransomware

In September 2023, MGM Resorts experienced a ransomware attack that disrupted operations across multiple Las Vegas properties. Attackers reportedly used social-engineering techniques to gain privileged access and then deployed ransomware that disabled hotel room keys, slot machines, and reservation systems (Verizon, 2025). Although MGM had implemented a formal zero-trust framework, investigators discovered that privileged-access controls were inconsistently applied, permitting lateral movement once credentials were compromised. The company's swift public disclosure and cooperation with federal agencies helped limit reputational damage, but the incident underscored the enduring vulnerability of human factors and the necessity for adaptive access governance.

These cases deliver clear lessons: vendor security cannot replace continuous internal monitoring, social engineering remains a powerful attack vector, and effective incident-response planning must encompass both technical containment and organizational resilience.

7. Directions for Future Research and Practice

The rapidly intensifying threat landscape calls for coordinated action from practitioners, researchers, and policymakers. Although each group has distinct responsibilities, all share the overarching objective of creating resilient and trustworthy digital ecosystems.

7.1. Strategies for Practitioners and Organizations

Enterprises must regard cybersecurity as a core business imperative rather than a peripheral technical function. Standard practices should include the deployment of zero-trust architectures, continuous threat-exposure management, and robust AI governance (NIST, 2023; IBM Security, 2025). Zero trust requires fine-grained identity verification, least-privilege access controls, and continuous monitoring of user and device activity. Continuous exposure management—supported by regular red-team exercises, automated dependency scanning, and rapid patching—helps reduce dwell time and limit the impact of successful intrusions.

Equally critical is cultivating a security-aware culture that begins with the board of directors and extends to every employee. Ongoing workforce development—such as cross-disciplinary training in AI security, privacy law, and secure coding—addresses both the talent shortage and the need for integrated decision making (ISC², 2025). Incentive programs should reward secure behavior and promote transparent reporting of near misses or vulnerabilities.

7.2. Strategies for Researchers

The academic and research community faces numerous open questions that require urgent attention. Developing robust adversarial AI models—systems resistant to manipulation and capable of explaining their decisions—remains a top priority (Goodman et al., 2024). The security characteristics of neuromorphic hardware, with its unconventional architectures and potential side-channel exposures, are largely uncharted. Post-quantum cryptography presents another major challenge: empirical data comparing candidate algorithms in large-scale, heterogeneous environments remain limited, and standardized benchmarks are scarce. Additional field studies and the creation of shared datasets are essential to validate defensive techniques and ensure reproducibility.

7.3. Strategies for Policy Makers

Governments must craft regulations that keep pace with technological innovation while avoiding unnecessary barriers to progress. Because cyber adversaries operate across borders, international cooperation is critical. Frameworks such as the European Union's NIS2 Directive and the U.S. Cyber Incident Reporting for Critical Infrastructure Act offer valuable starting points but require harmonization to enable effective cross-border enforcement (ENISA, 2025; CISA, 2023). Policymakers should also create incentives for secure design, including liability provisions for negligent software development and certification programs that reward vendors demonstrating strong security practices (European Commission, 2024). Clear guidelines for AI governance and data protection will help align industry practices with evolving societal expectations.

8. Conclusion

The cybersecurity arena is entering a phase of profound change. Adversaries now leverage artificial intelligence, exploit intricate supply-chain relationships, and target edge devices in ways that overwhelm traditional defenses. In turn, organizations are responding with AI-driven analytics, zero-trust architectures, adaptive security frameworks, and secure-by-design development practices. Despite these advances, technical limitations, regulatory gaps, human error, and economic constraints continue to provide openings for attackers.

The stakes are immense. Individual breaches already inflict multi-million-dollar losses, while critical infrastructure and personal privacy remain under persistent threat. In the coming years, the contest between offensive innovation and defensive adaptation will only accelerate. Broad deployment of quantum-resistant cryptography, explainable AI, and continuous threat-exposure management is poised to shape the next era of cybersecurity. Ultimately, sustained collaboration among practitioners, researchers, and policymakers will determine whether societies can outpace adversaries or face mounting disruption.

References

[1] Bhatt, S. I. (2025). Cybersecurity risks in connected medical devices: Mitigating threats to patient safety. *International Journal of Trend in Scientific Research and Development, 9*(2), 433–444. International Journal of Trend in Scientific Research and Development.

[2] CISA. (2023). *Secure by design, secure by default*. U.S. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/resources-tools/resources/secure-by-design

[3] Coveware. (2024). *MOVEit transfer vulnerability and global ransomware impact report*. Coveware Research. https://www.coveware.com

[4] CrowdStrike. (2025). *AI-powered cyberattacks: Emerging tactics and defensive strategies*. CrowdStrike Threat Report. https://www.crowdstrike.com

[5] Dhole, S. P. (2025). Latest trends and defensive strategies in cybersecurity: Emerging threats, research gaps, and future directions. International Journal of Trend in Scientific Research and Development, 9(5), 333–340. http://www.ijtsrd.com/papers/ijtsrd97506.pdf

[6] ENISA. (2025). *Technical implementation guidance on cybersecurity risk management measures (Version 1.0)*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

[7] Eraneos. (2025). *Preparing for the post-quantum era: Building crypto agility*. Eraneos Research Paper. https://www.eraneos.com

[8] European Commission. (2024). *Cyber Resilience Act: Strengthening cybersecurity rules for digital products*. Publications Office of the European Union. https://eur-lex.europa.eu

[9] European Data Protection Board. (2024). *Guidelines on data protection in cybersecurity monitoring*. EDPB Publications. https://edpb.europa.eu

[10] Gartner. (2024). *Adaptive security architecture for advanced threat defense*. Gartner Research. https://www.gartner.com

[11] Goodman, R., Patel, S., & Wong, A. (2024). Explainable artificial intelligence for cybersecurity: Opportunities and obstacles. *IEEE Security & Privacy, 22*(3), 47–56. https://doi.org/10.1109/MSEC.2024.1234567

[12] IBM & Ponemon Institute. (2025). *Cost of a data breach report 2025*. IBM Corporation. https://www.ibm.com/reports/cost-of-a-data-breach

[13] IBM Security. (2025). *AI-driven security operations: Leveraging machine learning for faster detection and response*. IBM Corporation. https://www.ibm.com/security

[14] ISC². (2025). *Cybersecurity workforce study 2025*. International Information System Security Certification Consortium. https://www.isc2.org

[15] Jariwala, M. (2025). The impact of AI and data analytics on project management information systems (PMIS). In Project management information systems: Empowering decision making and execution (pp. 117–160). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-0700-8.ch004

[16] Microsoft Security. (2025). *Large language models in cybersecurity: Early findings from enterprise deployments*. Microsoft Security Research. https://www.microsoft.com/security

[17] National Institute of Standards and Technology. (2023). *Zero trust architecture* (Special Publication 800-207). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-207

[18] PwC. (2025). *Cybersecurity governance in the boardroom: 2025 global survey*. PricewaterhouseCoopers. https://www.pwc.com

[19] Trustwave. (2025). *Salesloft-Drift supply chain attack report*. Trustwave SpiderLabs. https://www.trustwave.com

[20] Verizon. (2025). *2025 data breach investigations report*. Verizon Enterprise Solutions. https://www.verizon.com/business/resources/reports/dbir/

[21] World Economic Forum. (2025). *Global cybersecurity outlook 2025*. World Economic Forum. https://www.weforum.org

[22] Zhang, Z., Al Hamadi, H., Damiani, E., Chan, C. Y., & Taher, F. (2022). Explainable artificial intelligence applications in cyber security: State-of-the-art in research. *IEEE Access, 10,* 93113–93138. https://doi.org/10.1109/ACCESS.2022.3204051